ECS Configuration Change Request

1. Originator	2. Log Date:	3. CCR #:	4. Rev:	5. Tel:	6. Rm #:	7. Dept.
Henry Baez	10/6/00	00-0990	–	301-925-1025	2101D	SED

8. CCR Title: Install and run Distributed Denial of Service trojan detection tool on baseline Solaris systems in all DAACs.

9. Originator Signature/Date	10. Class	11. Type:	12. Need Date:
Henry Baez 10/6/2000	II	CCR	10/18/2000

13. Office Manager Signature/Date	14. Category of Change:	15. Priority: (If "Emergency" fill in Block 28).
James R Mather 10/6/2000	Initial ECS Baseline Doc.	Routine

16. Documentation/Drawings Impacted:	17. Schedule Impact:	18. CI(s) Affected:
910-TDA-003, 920-TDX-002, 914-TDA-146		910-TDA-003/920-TDX-002, 914-TDA-146

19. Release Affected by this Change:	20. Date due to Customer:	21. Estimated Cost:
5B	N/A	None - Under 100K

22. Source Reference: ☐NCR (attach) ☐Action Item ☐Tech Ref. ☐GSFC ☐Other:

23. Problem: (use additional Sheets if necessary)
The National Infrastructure Protection Center has developed a tool to check Solaris systems for most of the major Distributed Denial of Service (DDOS) tools found in the wild. DDOS attacks uses a number of systems to attack a network and saturated that network with so much traffic that the network is rendered un-useable. The attackers compromise systems at many locations and install trojan tools with out the knowledge of the owners of those systems. CERT, NASIRC, and other security organizations highly recommend that this software be run on all networked Solaris systems to detect the presents of the DDOS trojan.

24. Proposed Solution: (use additional sheets if necessary)
Load and run the executable, FIND_DDOS version 3.3, on baseline all DAAC Solaris 2.5.1 platforms. We recommend that the executable be put in a root-only automounted directoy for ease of execution.

This tool has been tested in the IDG Test Cell, Functionality Lab, and VATC machines with out any reported problems.

25. Alternate Solution: (use additional sheets if necessary)
The outside or perimeter of ECS networks could be strengthen with firewalls that would offer protection to all the platforms.

26. Consequences if Change(s) are not approved: (use additional sheets if necessary)
ECS runs the risk that intruders will use ECS compromise systems to attack other network and generating so much traffic that not only the attacked network but also the ECS network is affected. This happened to several university systems in California in February.

27. Justification for Emergency (If Block 15 is "Emergency"):

28. Site(s) Affected: ☐EDF ☒PVC ☐VATC ☒EDC ☒GSFC ☒LaRC ☒NSIDC ☒SMC ☐AK ☐JPL ☐EOC ☐IDG Test Cell ☐Other

29. Board Comments:	30. Work Assigned To:	31. CCR Closed Date:

32. EDF/SCDV CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
33. M&O CCB Chair (Sign/Date): 10/17/00	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ECS
34. ECS CCB Chair (Sign/Date):	Disposition: Approved App/Com. Disapproved Withdraw Fwd/ESDIS ERB Fwd/ESDIS

ORIGINAL